CLAIMS

1. A method for securely transmitting data from a sending communication device to a receiving communication device comprising:

storing at least one private key in a receiving communication device in a secure portion;

receiving at a sending communication device at least one public key from said receiving communication device;

using at said sending communication device said at least one public key to transform clear digital data into encrypted digital data;

said sending communication device forwarding said encrypted digital data to said receiving communication device; and

using said at least one private key at said receiving communication device to decrypt said encrypted digital data.

2. The method of claim 1 wherein said secure portion comprises a processor.

3. The method of claim 2 wherein said processor comprises an Application Specific Integrated Circuit (ASIC) having said secure portion for holding said at least one private key.

4. The method of claim 1 wherein said secure manner comprises a means for tamper proofing.

5. The method of claim 4 wherein said means for tamper proofing erases said at least one private key upon an indication of tampering.

6. The method of claim 1 wherein said using said at least one private key at said receiving communication device to decrypt said encrypted digital data further comprises:

obtaining said at least one private key from a processor.

7. The method of claim 1 wherein said receiving communication device determines the authenticity of said at least one public key.

8. The method of claim 1 wherein said secure portion comprises a tamper proof ASIC.

9. The method of claim 8 wherein authentication is required for access to said secure portion.

10. The method of claim 9 wherein said authentication utilizes encryption.

11. A system for securing data communications between a sending communication device and a receiving communication device comprising:

a sending communication device comprising:

said sending communication device comprising a first processor comprising a sender's secure portion, said sender's secure portion having at least one sender's private key;

said sending communication device a first memory medium comprising a receiver's public key and a first module configured to forward at least one sender's public key to a receiving communication device associated with said at least one sender's private key;

an interconnection fabric configured to couple said sending communication device with said receiving communication device;

said receiving communication device comprising:

a second memory medium comprising a second module configured to obtain said at least one sender's public key from said sending communication device;

a second processor comprising a secure portion, said secure portion having at least one receiver's private key which complements said at least one receiver's public key;

a first Analog to Digital Converter (ADC) associated with said sending communication device, said first ADC configured to obtain analog data from a user and convert said analog data to digital data;

said first module configured to transform said digital data to encrypted data using said at least one receiver's public key and provide said encrypted data to said receiving communication device via said interconnection fabric;

said receiving communication device configured to utilize said at least one receiver's private key from said receiver's secure portion to transform said encrypted data back to said digital data;

said receiving communication device having a second Digital to Analog Converter (DAC) configured to transform said digital data to resulting analog data.

12. The system of claim 11 wherein said first processor and said second processor each comprise at least one Application Specific Integrated Circuit (ASIC).

13. The system of claim 11 wherein said first module configured to forward said at least one sender's public key to said receiving communication device encapsulates said sender's public key in a data header.

14. The system of claim 11 wherein said receiving communication device authenticates said sender's public key.

15. The system of claim 14 wherein said authentication depends upon verification of a sender's digital signature associated with said at least one sender's public key.

16. The system of claim 11 wherein said sending communication device authenticates said receiver's public key.

17. The system of claim 16 wherein said authentication depends upon verification of a receiver's digital signature associated with said at least one receiver's public key.

18. The system of claim 11 wherein said analog data comprises voice data provided by said user.

19. The system of claim 11 wherein said sending communication device and said receiving communication device are telephones.

20. The system of claim 11 wherein said receiving communication device further comprises:

a second ADC configured to obtain an analog data reply from a receiving user at said receiving communication device and convert said analog data reply to a digital data reply;

said second module configured to transform said digital data reply to an encrypted data reply using said at least one sender's public key and forward said encrypted data reply to said sending communication device;

said sending communication device configured to obtain said at least one sender's private key from said secure portion and utilize said at least one sender' private key to transform said encrypted data reply to said digital data reply;

said sending communication device having a first DAC configured to transform said digital data reply to an analog data reply.

21. An apparatus for sending secure data to a receiving apparatus comprising:

a first Analog to Digital Converter (ADC) configured to obtain an analog data signal and convert said analog data signal to digital data;

a first Application Specific Integrated Circuit (ASIC) comprising a secure portion, said secure portion having at least one sender's private key;

a first memory medium comprising a means for obtaining a receiver's public key from a receiving apparatus and using said at least one receiver's public key to transform said digital data to encrypted data;

a communication link for transmitting said encrypted data to a said receiving apparatus.

22. The apparatus of claim 21 further comprising:

said first memory medium comprising a means for transmitting at least one sender's public key which complements said at least one sender's private key to said receiving apparatus.

23. The apparatus of claim 21 wherein said sending apparatus comprises a telephone.

24. The apparatus of claim 23 wherein said telephone further comprises a means for determining if said receiving apparatus is secure.

25. The apparatus of claim 21 further comprising:

an interface configured to convey to a user when said communication link is secure.

26. The apparatus of claim 25 wherein said interface comprises an indicator light for conveying whether said communication link is secure.

27. The apparatus of claim 21 wherein said first ASIC comprises a means for tamper proofing.

28. The apparatus of claim 27 wherein said means for tamper proofing erases said at least one sender's private key upon an indication of tampering.

29. The apparatus of claim 21 wherein access to said secure portion of said ASIC requires authentication.

30. In a computer system, a method for receiving secure communication data comprising:

obtaining encrypted data;

obtaining at least one sender's public key from a sender of said encrypted data;

providing at least one receiver's public key to a sending communication device;

using said at least one receiver's private key from a receiver's secure portion to transform said encrypted data into clear digital data;

converting said clear digital data to clear analog data;

playing said clear analog data to a receiving user;

obtaining reply analog data from said receiving user;

converting said reply analog data to reply digital data;

obtaining at least one sender's public key;

using said at least one sender's public key to transform said reply digital data to encrypted reply data;

forwarding said encrypted reply data to said sender.

31. The method of claim 30 wherein said secure portion comprises an Application Specific Integrated Circuit (ASIC).

32. The method of claim 30 wherein said secure portion comprises a tamper proofing mechanism.

33. The method of claim 32 wherein said tamper proofing mechanism comprises:

determining if an unauthorized user attempts to access said at least one receiver's private key;

deleting said at least one receiver's private key from said secure portion if said determination is affirmative.

34. The method of claim 33 wherein said secure portion comprises a secured processor.